<u>Amendments to the Claims:</u>

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-12 (Canceled)

13. (Currently Amended) A method for enciphering a sequence of clear text data values comprising:

    a. nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets wherein each of the plurality of large random secrets is a random value and further wherein the plurality of shuffled large random secrets are each a random value <u>and wherein the plurality of mixing keys are random and secret</u>;

    b. performing an exclusive OR on the plurality of shuffled large random secrets to produce a plurality of large random pads <u>wherein the plurality of large random pads have less entropy than the plurality of shuffled large random secrets</u>;

    c. circularly rotating the values of each of the plurality of large random pads according to a plurality of random rotation values thus forming a plurality of rotated large random pads <u>wherein the plurality of random rotation values are random and secret</u>;

    d. randomly shuffling a portion of each of the plurality of rotated large random pads according to a plurality of working keys thus forming a

2

plurality of randomly rotated and randomly shuffled large random pads wherein the plurality of working keys are random and secret;

e. performing an exclusive OR function on the plurality of randomly rotated and randomly shuffled large random pads to produce a final pad wherein the final pad has less entropy than the plurality of randomly rotated and randomly shuffled large random pads;

f. selecting a portion of the final pad to form a finite key stream; and

g. performing an exclusive OR function with the finite key stream with the sequence of clear text data values.

14. (Previousy Amended) The method according to Claim 13 further comprising substituting a value within each of the plurality of shuffled large random secrets with a new random value using a plurality of substitution keys thus forming a plurality of nested shuffled and substituted large random secrets.

15. (Original) The method according to Claim 13 further comprising substituting a value within each of the plurality of large random secrets with a new random value using a plurality of substitution keys thus forming a plurality of substituted large random secrets.

16. (Previously Amended) The method according to Claim 13 further comprising selecting a series of portions of the final pad to form the finite key stream.

3

17. (Previously Amended) The method according to Claim 13 further comprising transmitting the plurality of large random secrets, a plurality of substitution keys, the plurality of mixing keys, the plurality of working keys and the plurality of rotation values from a central server.

18. (Previously Amended) The method according to Claim 13 further comprising transmitting the plurality of large random secrets, a plurality of substitution keys, the plurality of mixing keys, the plurality of working keys and the plurality of rotation values from a storage device.

19. (Currently Amended) A method for deciphering enciphering a sequence of cipher text data values comprising:

    a. nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets wherein each of the plurality of large random secrets is a random value and further wherein the plurality of shuffled large random secrets are each a random value and wherein the plurality of mixing keys are random and secret;

    b. performing an exclusive OR on the plurality of shuffled large random secrets to produce a plurality of large random pads wherein the plurality of large random pads have less entropy than the plurality of shuffled large random secrets;

    c. circularly rotating the values of each of the plurality of large random pads according to a plurality of random rotation values thus forming a

plurality of rotated large random pads <u>wherein the plurality of random rotation values are random and secret</u>;

d.   randomly shuffling a portion of each of the plurality of rotated large random pads according to a plurality of working keys thus forming a plurality of randomly rotated and randomly shuffled large random pads <u>wherein the plurality of working keys are random and secret</u>;

e.   performing an exclusive OR function on the plurality of randomly rotated and randomly shuffled large random pads to produce a final pad <u>wherein the final pad has less entropy than the plurality of randomly rotated and randomly shuffled large random pads</u>;

f.   selecting a portion of the final pad to form a finite key stream; and

g.   performing an exclusive OR function with the finite key stream with the sequence of cipher text data values.

20. (Previously Amended) The method according to Claim 19 further comprising substituting a value within each of the plurality of shuffled large random secrets with a new random value using a plurality of substitution keys thus forming a plurality of nested shuffled and substituted large random secrets.

21. (Previously Amended) The method according to Claim 19 further comprising selecting a series of portions of the final pad to form the finite key stream.

22. (Previously Amended) The method according to Claim 19 further comprising transmitting the plurality of large random secrets, a plurality of substitution

keys, the plurality of mixing keys, the plurality of working keys and the plurality of rotation values from a central server.

23. (Previously Amended) The method according to Claim 19 further comprising transmitting the plurality of large random secrets, a plurality of substitution keys, the plurality of mixing keys, the plurality of working keys and the plurality of rotation values from a storage device.

Claims 24-29 (Canceled)